Juan Miguel Cano

Rodolfo Gonzalez

Splunk Dashboard Query and Alert

(Match to color is key to understanding the description of the query)

ATTACK MAP (Mock Map)

```
 | makeresults
| eval Country="United States", Count=100
| append [ | makeresults
| eval Country="Iran", Count=15 ]
| append [ | makeresults
| eval Country="North Korea", Count=75 ]
| append [ | makeresults
| eval Country="Russia", Count=50 ]
| append [ | makeresults
| eval Country="China", Count=25 ]
| geom geo_countries featureIdField="Country" countfield="Count"
```

PRIME TIME DEFENSE PIE CHART

ALL PROCESSES

*

PRIME TIME DEFENSE LINE CHART

REAL-TIME OF ALL PROCESSES

*

ATTACK DETECTED / SOURCE TYPE / EVENT COUNT

REAL-TIME

index="main"

(host="RISK-ANALYST1" OR host="ACCOUNTING1" OR host="ACCOUNTING2" OR host="CFO-LAPTOP" OR host="ip-10-0-0-175" OR host="linsecurity")

(sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" OR sourcetype="WinEventLog:Security" OR sourcetype="linux_secure" OR sourcetype="apache_error")

AND (

(

sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" AND

"Process Create" AND

```
        (CommandLine="*powershell.exe*" OR CommandLine="*cmd.exe /c*")
    )
        OR
        (
        sourcetype="WinEventLog:Security" AND
        (EventCode=4625 OR EventCode=4740)
        )
        OR
        (
        sourcetype="linux_secure" AND
        "Failed password" AND
        NOT user="known_good_user"
        )
        OR
        (
        sourcetype="apache_error" AND
        (
        "client denied by server configuration" OR
        "File does not exist" OR
        "script not found or unable to stat"
        )
        )
)
| eval AttackDetected=if(
```

```
        match(_raw, "Process Create|EventCode=4625|EventCode=4740|Failed password|client denied by server configuration|File does not exist|script not found or unable to stat"),

        "Yes",

        "No"

  )

| stats count as EventCount by host, AttackDetected, sourcetype

| sort - EventCount
```

This query was used as an alert and dashboard to monitor incoming attacks, source type, and event count.

It filters events based on certain conditions related to different source types:

1. For Sysmon Operational logs on Windows hosts (EventCode 1- Process Create), it looks for processes created with PowerShell or cmd.exe.

2. For Security logs on Windows hosts (EventCode 4625 or 4740), it looks for failed login attempts.

3. For Linux secure logs, it looks for failed password attempts from users other than “known_good_user.”

4. For Apache error logs, it looks for specific error messages indicating denied access or missing files.

After filtering, it evaluates if an attack is detected based on the presence of specific keywords in the raw event data and assigns “Yes” or “No” to the “AttackDetected” field.

Finally, it calculates the count of events grouped by host, AttackDetected, and sourcetype, sorting the results by EventCount in descending order.

This query helps to identify potential security incidents or anomalies across different types of logs and hosts.

Alerts

A total comprehensive Alert (too large for Dashboard Visualization)

```
(index="main" (host="RISK-ANALYST1" OR host="ACCOUNTING1" OR host="ACCOUNTING2" OR host="CFO-LAPTOP" OR host="ip-10-0-0-175")

AND

 (

   (sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" AND ("Process Create" AND (CommandLine="*powershell.exe*" OR CommandLine="*cmd.exe /c*")))
OR

   (sourcetype="WinEventLog:Security" AND (EventCode=4625 OR EventCode=4740))
OR

        (sourcetype="linux_secure" AND "Failed password" AND NOT user="known_good_user") OR

        (sourcetype="apache_error" AND ("client denied by server configuration" OR "File does not exist" OR "script not found or unable to stat"))

))

| eval AttackDetected=if(match(_raw, "Process Create|EventCode=4625|EventCode=4740|Failed password|client denied by server configuration|File does not exist|script not found or unable to stat"), "Yes", "No")

| table _time, host, AttackDetected, sourcetype, _raw

| sort - _time
```

This query is for use with Splunk, log management, or SIEM (Security Information and Event Management) systems. It is designed to filter and analyze security-related events from various sources within our AWS Network environment.

1. **Index Specification:** It searches within the “main”index for logs coming from a set of specific hosts (‘RISK-ANALYST1’, ‘ACCOUNTING1’, ‘ACCOUNTING2’, ‘CFO-LAPTOP’, and ‘ip-10.0.0.175’). This narrows the search to logs generated by these critical or sensitive systems.

2. **Source and Event Filtering:**

- Filters for logs from the Windows Sysmon Operational log with events related to process creation ‘ ”Process Create” ’) that involve either PowerShell (‘powershell.exe’) or Command Prompt (‘cmd.exe /c’). This is typically used to identify potentially malicious script executions.

- Includes Security logs from Windows with Event Codes 4625 (failed logon attempts) and 4740 (account lockout), indicating possible brute-force attacks or account compromise attempts.

- Search for failed login attempts (‘ ”Failed password” ‘) in Linux secure logs, excluding ones from a ‘known_good_user’, helping to identify unauthorized access attempts.

- Looks for specific Apache server error messages indication access control issues or attempts to access non-existent resources or scripts, which might suggest probing or attack attempts.

3. **Attack Detection Logic:** It uses an ‘eval’ command to add a field named ‘AttackDetected’, which flags each event as “Yes” if it matches any of the criteria described above, indicative of potential security incidents.

4. **Output Formatting:**

- The ‘table’ command structures the output into a table format, showing the time of the event (‘_time’), the host from which the log originated, whether an attack was detected (‘AttackDetected’), the type of log source(‘sourcetype’), and the raw log entry (‘_raw’).

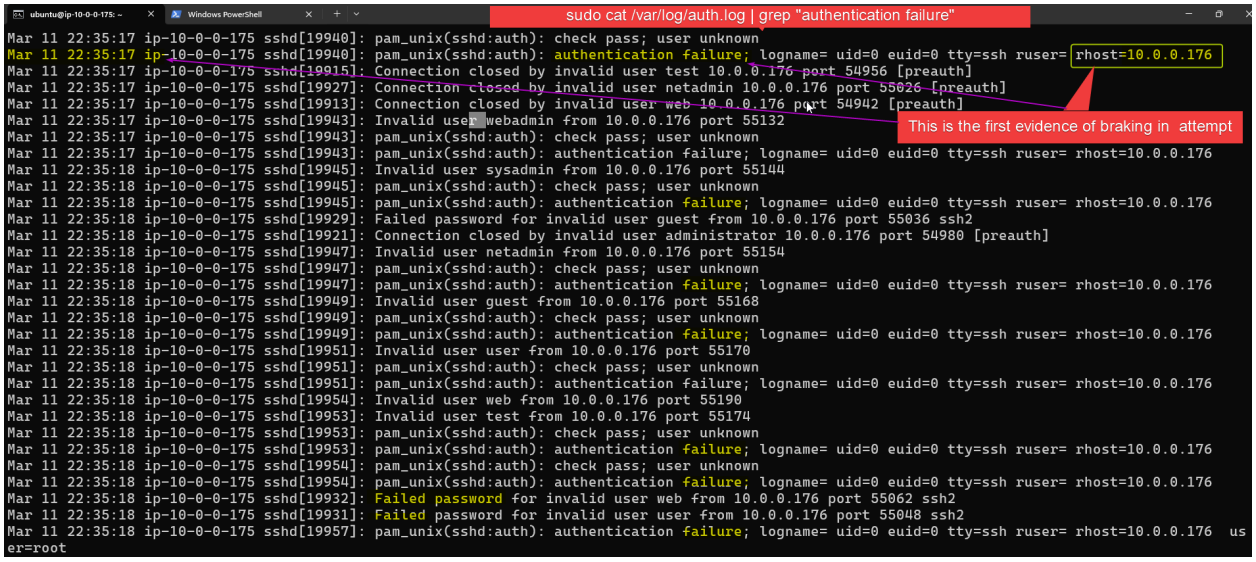
- It sorts the results in descending order by time (‘- _time’), showing the most recent events first.

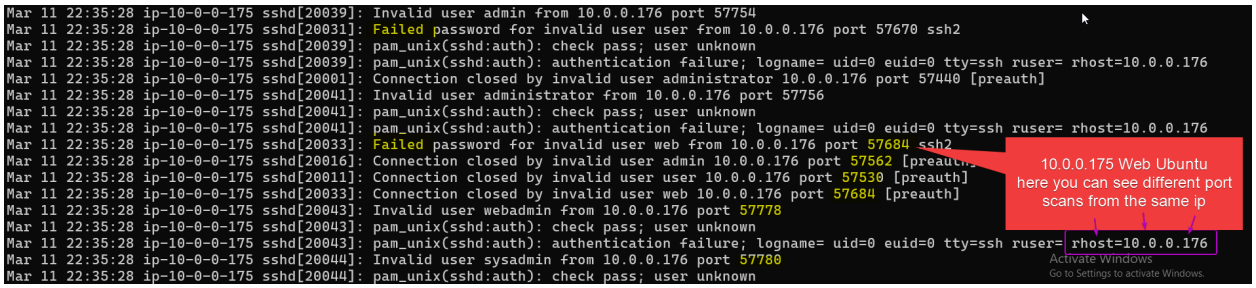
This query is a powerful tool for a security analyst to quickly identify potential security incidents across different systems and log types by highlighting critical events that may indicate attack attempts or system compromises.

I went to the 10.0.0.175 and searched the logs pertaining to failed logged-in attempts with following commands and this is the first part:.

I tries do check the logs in Bob computer but he does not have the credential to do so.

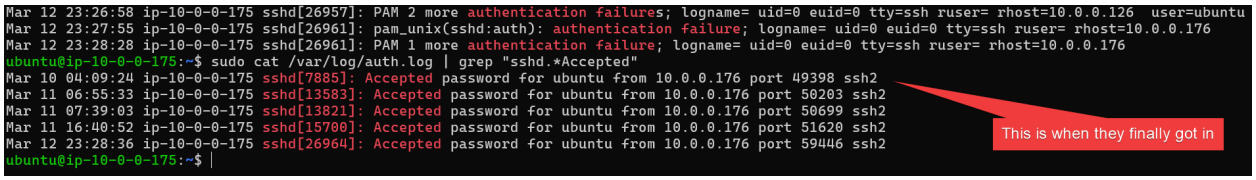
sudo cat /var/log/auth.log | grep "authentication failure"





Now I check when they actually get in with the following command:

sudo cat /var/log/auth.log | grep "sshd.*Accepted"



Here you can see that 10.0.0.126 is also attempting to ssh.

https://docs.google.com/presentation/d/1zaCPbFnbqMIyAIHtUVqfTDB549ItnrttLIhiqUStrbg/edit?usp=sharing